U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

January 9, 2024

BY ECF

The Honorable Eric R. Komitee
United States District Judge
United States District Court
Eastern District of New York
225 Cadman Plaza
Brooklyn, New York 11201

Re: *Joshua Adam Schulte v. United States of America*, 22 Civ. 766 (EK)

Dear Judge Komitee:

The United States Attorney's Office for the Southern District of New York respectfully submits this letter in opposition to petitioner Joshua Adam Schulte's petition to modify his conditions of confinement to the extent that request would contravene Special Administrative Measures ("SAMs") imposed on Schulte to prevent his disclosure of classified information. As Schulte stipulated at trial, "As a result of [Schulte's] employment at the Central Intelligence Agency ["CIA"], he was privy to and remains aware of sensitive national defense information beyond what he is charged with disclosing or attempting to disclose . . . , the disclosure of which would be extremely damaging to national security." (GX 3010 (stipulation), attached as Exhibit A). As recently as last year, Schulte threatened in a court filing that he "retains so much real national defense information that would be extremely damaging to the national security of the United States," and that "[i]f and when Mr. Schulte ever decides to wage a war against the United States, he could easily cause true, catastrophic damage." *Infra* at 10.

As described further below, Schulte has repeatedly disclosed and attempted to disclose that sensitive national security information, before his arrest and while incarcerated. Schulte used his contact with friends and family members and with other inmates to provide classified information and protected discovery materials to reporters, to procure contraband jailhouse cellphones, to set up anonymous and encrypted email and social media accounts, and the plot and carry out a campaign to disclose additional damaging, and potentially life-threatening, classified information in a destructive fit of retaliation. The SAMs have been reimposed based on a specific annual consideration of that risk, accompanied by a renewed personal certification of their necessity by the Director of the CIA, as required by the Code of Federal Regulations and the Justice Manual.

Accordingly, the continued imposition of SAMs is necessary and appropriate to protect the public and the national security of the United States.[1]

1. Schulte's Work as a Developer at the CIA

Schulte began working for the CIA in approximately 2012 as a software developer in the Center for Cyber Intelligence ("CCI"), which conducts offensive cyber operations, that is, cyber espionage relating to foreign governments or terrorist organizations. (Tr. 449-50, 1361, 1661.)[2] Until approximately March 2016, Schulte was assigned to the Operations Support Branch ("OSB"). (Tr. 1359-60, 1620.)[3] OSB was particularly focused on counterterrorism, developing cyber tools designed to gain access to computer networks and gather intelligence information. (Tr. 466, 1360-61, 1426.) OSB's tools were used in, among other thing, human-enabled operations or asset-enabled operations—that is, cyber operations that involved a person with access to the computer network being targeted by the cyber tool. (Tr. 1360, 1620.) In March 2016, Schulte was moved to the Remote Development Branch ("RDB") as a result of personnel issues. (GX1046; Tr. 486-90, 1392.)

In addition to being a developer, Schulte was also, for a time, one of the administrators of the suite of development programs produced by Atlassian Corporation that OSB and other development branches used to develop cyber tools. (Tr. 471-72, 1363, 1374, 1621.) Schulte was also one of the OSB developers who administered a server used by OSB to design and test cyber tools. (Tr. 1375-76.)

2. Schulte's Administrator Privileges Are Revoked and He Lies About His Abuse of Privileges

In April 2016, Schulte abused his Atlassian administrator powers to grant himself administrator privileges to an OSB project for which he had been made an ordinary user as a result of his move from OSB to RDB. (GX1061; GX1062; GX1207-65, GX1207-97, GX1703-1 at 9, GX1704-1 at 1; Tr. 495-99, 500-12, 518-23, 1396-1403.) When Schulte first discovered that his project administrator status had been removed, he confronted a colleague who had implemented the permissions change, falsely claimed to have gotten approval from a supervisor to have his permissions restored, and threatened that he would "eventually get access back to the [project] and that access should just be enabled now." (GX1062; Tr. 1396-97.) Then, after Schulte unsuccessfully sought to be restored as a project administrator through a series of emails with

---

[1] The undersigned understand that Schulte's petition in this case pursuant to 28 U.S.C. § 2241 expressly disclaims any challenge to the SAMs, instead asserting that the Bureau of Prisons has imposed additional conditions on him that are not required by the SAMs. *See* Petition at 16.

[2] In this letter, references to "Tr." are to the transcript of the 2022 trial before the Honorable Jesse M. Furman in *United States v. Joshua Adam Schulte*, 17 Cr. 548 (JMF) (S.D.N.Y.); references to "GX" are to Government exhibits at that trial; "DX" are to defense exhibits at trial; and "D.E." are to entries in the electronic docket.

[3] OSB and its sister development branches were under a division called the Applied Engineering Division ("AED").

additional supervisors, he simply used his Atlassian administrator privileges to make himself an administrator for the OSB project. (GX1061; GX1207-65, GX1207-97, GX1703-1 at 9, GX1704-1; Tr. 495-99, 1398, 1401-03.)

Schulte's abuse of administrator privileges was detected, and CCI leadership directed that Atlassian administrator privileges would immediately be transferred from developers to another division, the Infrastructure Support Branch ("ISB"). (GX1064; GX1207-7, GX 1207-11, GX1207-18; GX1207-21; GX1207-95, GX1207-96, GX1207-98, GX1207-99; GX1703-1 at 2-3 & 22-27; Tr. 522-24, 742-43, 746, 831-38, 1377-78, 1406-09.)

The Monday after the developers' Atlassian administrator privileges were revoked and transferred to ISB administrators, Schulte was given a warning about self-granting administrator privileges that had previously been revoked. (GX1066; GX1095; Tr. 525-29.) Schulte lied about his threat that he would "eventually get access back" to the project and claimed he said that he was going to add his own access back unless someone with authority advised him not to; and claimed that he thought the removal of his permissions was unauthorized. (GX1095; Tr. 528.)

3. Schulte Uses a Secret Administrator Session to Steal the CIA's Cyber Tool Library

Before Schulte's Atlassian administrator privileges were revoked, he opened a secret administrator session on OSB's server (GX1703-1 at 15-20, GX1209-13, GX1203-18; Tr. 816-20), which was also used to host an Atlassian tool called "Confluence" as a virtual server.[4] (Tr. 1376.) The Confluence virtual server running on OSB's server had access to the network location where backups of AED's development suites were stored, which contained extensive documentation about the CIA's cyber tools. (GX1207-36; Tr. 766, 814-16, 1382-84.)

After Schulte's and the other developers' Atlassian administrator privileges were transferred to ISB, Schulte lied to his supervisor and claimed that "I verified that all private keys with access have been destroyed/revoked." (GX1063.) Shortly before making this representation, Schulte tested his administrator access to the OSB server using a private key and found that it was still active, and Schulte was still running an administrator session on OSB's server when he made the representation. (GX1703-1 at 32, GX1209-17; Tr. 841-42.)

Already angry about the personnel issues that led to his reassignment from OSB to RDB and the reassignment itself, Schulte was livid about the revocation of his Atlassian administrator privileges, and immediately began testing his ability to access restricted parts of the CIA cyber tool development network in order to steal AED's cyber tool library. (GX1203-18; GX1202-7; GX1209-09; GX1209-13, GX1703-1 at 11-12 & 15-20, GX1704-1 at 32-34, GX3501-1; Tr. 778, 811-14, 816-20, 1148-49.) Although Schulte could not access the network location where Atlassian backups were stored after the removal of his Atlassian privileges (Tr. 1410-11), he was able to use his administrator session on the OSB server to view the Confluence virtual server and review, edit, and delete log files. (GX1209-8; GX1703-1 at 36-37 & 39, GX1203-43; Tr. 845-49.)

[4] A virtual server is a type of virtual computer, which is a software representation of a computer that mimics the operations and functionality of a physical computer. (Tr. 1376-77.)

On April 20, 2016—only six days after abusing his administrator privileges and only two days after being admonished for doing so—after other developers had left the office, Schulte used his OSB server administrator session to execute a complicated series of maneuvers on the CIA network to restore his Atlassian administrator privileges, break in to the backups, steal copies (the "Stolen CIA Files"), revert the network back to its prior state, and delete hundreds of log files in an attempt to cover his tracks. (GX1201-16; GX1202-18; GX1202-19; GX1202-20; GX1202-21; GX1203-1; GX1203-2; GX1207-27; GX1207-30; GX1703-1 at 47-51, 53-55, 61, 63-64, 66, 68-90; Tr. 762-63, 854-93, 1083-84, 1089, 1379-81, 1624.)

4. Schulte Transmits the Stolen CIA Files to WikiLeaks and Securely Deletes Data from His Home Computer

Between April 18 and May 5, 2016, Schulte took a number of steps to transmit the Stolen CIA Files to WikiLeaks: Schulte updated his versions of Tails (an operating system that boots from an external media device and is designed to leave no forensic trace of the user's activities) and the Tor browser (an encrypted, anonymizing network that makes it difficult to intercept or trace internet communications that can access the "dark web") on his home computer—both tools recommended by WikiLeaks to potential leakers. (GX1403-7; GX1704-1 at 38-45 & 52; Tr. 1104-10, 1308-13; DX1409 rows 4873-8000.) Schulte also researched, downloaded, and tested different tools for secure data deletion—the kind of data deletion that frustrates forensic recovery efforts—another tactic recommended by WikiLeaks (GX1305-9; GX1402-8; GX1404-1; GX1404-2; GX1404-15; GX1704-1 at 50, 58-69; Tr. 1111-14, 1120-22, 1166-67, 1175-76); and researched fast hash algorithms, a mathematical tool used to confirm error-free data transmission. (GX1704-1 at 68, GX1305-8; Tr. 1170-71.) On May 5, 2016, having transmitted the Stolen CIA Files to WikiLeaks, Schulte wiped and reformatted his home computer's internal hard drives. (GX1704-1 at 72 & 73; Tr. 1173-77, 1311-12, 1315.) Schulte also had several other external hard drives that had been securely wiped by the time the Federal Bureau of Investigation ("FBI") seized them from his apartment in 2017. (GX 1608-1615; Tr. 1167-69, 1315.)

Schulte resigned from the CIA in late 2016 and relocated to Manhattan. In the time period between leaking the Stolen CIA Files and resigning, Schulte repeatedly embellished and escalated his false claims about his April 2016 abuse of administrator privileges, falsely claimed he was retaliated against for reporting personnel issues, falsely accused colleagues of misconduct, and again misused project administrator privileges to exclude OSB developers from another OSB cyber tool development project. (GX1080; GX1093; GX1096; Tr. 548-58, 667-72.) One of Schulte's supervisors, increasingly exasperated by Schulte's obstreperous conduct, explained that "I was frustrated by the fact that you kept trying to obtain your admin privileges over the [OSB development] project after being told not to do so, not to be [ ] reinstating your admin privileges and it kept coming up. And as a supervisor, when we asked you not to do that and you continued to do it, it became a problem. It was very frustrating." (Tr. 681.) In a meeting with one of the heads of CCI, where Schulte was warned that he could be fired for abusing administrator privileges, Schulte boasted, threatened, or both, that "I could restore my privileges if I wanted to, you know I could do that." (Tr. 1677.)

5. WikiLeaks Releases Data from the Stolen CIA Files, Causing Instant Devastation to the CIA's Cyber Operations

On March 7, 2017, WikiLeaks began publishing classified data from the Stolen CIA Files. (GX1.) Between March and November 2017, there were a total of 26 disclosures of classified data from the Stolen CIA Files, which WikiLeaks denominated as Vault 7 and Vault 8 (the "WikiLeaks Disclosures"). (Tr. 108, 112, 473-75, 1363-64, 1650-51.)

The impact on the CIA was immediately catastrophic. The network used to develop cyber tools was disconnected and the network and every external device connected to it were seized by the FBI. (Tr. 572-74, 1365; *see also* Tr. 130-31.) Personnel involved in cyber operations had no computer equipment for cyber development. (Tr. 1365.) Resources were diverted from developing tools for cyber operations to assessing the extent of the intrusion and the risk and impact of additional disclosures. (Tr. 572-73, 1364.) Further cyber operations were halted and previous and ongoing operations were at risk of exposure. (Tr. 575, 1366-67, 1651-52, 1686.) Cyber tools had to be rebuilt and redesigned. (Tr. 478, 575, 1364.) As described by one of the then-heads of CCI, the effect of the WikiLeaks Disclosures was a "digital Pearl Harbor. We were dead in the water." (Tr. 1681; *see also* Tr. 112-13.)

6. Schulte Continues His Efforts to Leak Classified Information and Protected Discovery Materials from Prison as Part of an "Information War" Against the U.S. Government

Schulte was ultimately arrested and remanded to the Metropolitan Correctional Center ("MCC") after having bail revoked for violating the terms of his release prohibiting Schulte from using the internet. (D.E. 22, 26 at 16.) In approximately April 2018, Schulte sent a copy of the affidavit in support of the warrant to search his apartment, which was subject to a discovery protective order (the "Protective Order"), to reporters with *The Washington Post* and *The New York Times*. In recorded prison telephone calls on April 17, 2018, Schulte discussed the information he had provided to the reporters with family members, and Schulte's family members' discussions with reporters on his behalf. Schulte's family members also arranged three-way conference calls with a reporter and on one of those calls, Schulte noted that the search warrant affidavit was subject to the Protective Order.

On May 15, 2018, articles were published in *The New York Times* and *The Washington Post* in which the authors described having reviewed the search warrant affidavit and described some of the allegations. At a court conference on May 18, 2018, the Honorable Paul A. Crotty, who was then presiding over the prosecution, admonished Schulte of the terms of the Protective Order, and Schulte acknowledged, "I understand." Despite the Court's admonishment, Schulte continued his plans to disclose protected discovery materials and classified information.

In the summer and fall of 2018, Schulte made plans to wage an "information war" against the United States Government to influence his criminal case through the media and to retaliate against his prosecution and perceived grievances against the CIA. In furtherance of this campaign, Schulte obtained access to contraband cellphones (Tr. 1712-20) that he used to create anonymous, encrypted email and social media accounts. (GX820-434 & -436; GX823; GX1303-11, -44, -50, & -63; Tr. 1752, 1831-35, 1853-57.)

Schulte documented his planned campaign in handwritten journals. In an entry dated August 8, Schulte wrote: "If govt doesn't pay me $50 billion in restitution & prosecute the criminals who liked to the judge and presented this BS case then I will visit every country in the world and bear witness to the treachery that is the USG [United States Government]. I will look to breakup diplomatic relationships, close embassies, end U.S. occupation across the world..." (GX809 at 2.) On August 14, Schulte wrote: "Got to use last night," referring to a contraband cellphone; "[t]he way is clear. I will set up a wordpress … From here, I will stage my information war." Schulte wrote about releasing posts and articles on social media as he wrote them. (GX809 at 3.)

In an "article" Schulte was writing about his various grievances against the government, he wrote: "The FBI, in all its brilliance, has just taken a senior engineer with intimate knowledge of the NSA, CIA, and all projects and operations he's worked on, including names of assets, specifics of covert actions . . . current and future targets, vulnerabilities . . . and names of intelligence community employees . . . and they have arrested him for a crime they know he didn't commit . . . . Does that sound like the most intelligent move, really? Obviously this isn't intended as a threat . . . . Essentially, it's the same as taking a soldier in the military, handing him a rifle, and then begin beating him senseless to test his loyalty and see if you end up getting shot in the foot or not. It just isn't smart." (GX820-430 & -431.)

Schulte continued to document his plans in an entry dated August 21, a checklist of actions for furthering his information war, avoiding detection, and deleting evidence. (GX809 at 5.) Schulte's list included deleting emails and documents from one of his anonymous accounts (johnsmith); creating new logins and passwords for accounts; creating a new encrypted email account; setting up new WhatsApp, Signal, and Telegram accounts with different phone numbers; resetting his contraband cellphone and cleaning off the apps; and changing the IMEI associated with his Samsung contraband cellphone. (*Id*.) Schulte learned that the FBI had learned the IMEI of one of his other cellphones by subpoena, and worried that the IMEI could be used to identify his accounts. (*Id*.) The following day, Schulte used a random password generator to create new passwords for his email and social media accounts. (GX809 at 6; Tr. 1833-34.)

On August 23, 2018, Schulte wrote about transitioning to his new encrypted email accounts and cleaning the contraband cellphone. (GX809 at 7.) Schulte also noted that he had started emailing a reporter from *The Washington Post*. (*Id.*) Using a messaging app and an anonymous email account, Schulte communicated with the reporter about his prosecution, pretending to be one of his own family members and a friend of the family. (GX812, GX822-1.) In an email dated September 24, 2018, Schulte emailed the reporter a search warrant affidavit that had been produced in discovery subject to the Protective Order, along with Schulte's comments on the affidavit. Schulte's criticisms of the affidavit's allegations included classified information about the CIA's cyber tool development network and the number of employees in CIA cyber intelligence groups. GX812 at 3; Tr. 1670-71.) In addition to emailing the reporter, Schulte attempted to use the contraband cellphones to transmit his discovery materials to WikiLeaks, but was unable to. His journal entry for September 12, 2018 includes the note, "DL disc UL WL," meaning "download discovery, upload to WikiLeaks." (GX809 at 15; *see also* Tr. 1754-56, 1799-1801.)

Throughout August and September, Schulte drafted blog posts and tweets. In these, Schulte pretended to be one of his own former CIA colleagues and falsely claimed his innocence. (GX809

at 8-13.) These draft tweets and blog posts contained classified information about CIA cyber tools and operations. Schulte sought to authenticate his assumed identity as a CIA developer by revealing information about a particular cyber tool called Bartender, including details of Bartender's operation and information that would publicly associate Bartender with a piece of malware that had been found by security professionals, but had never been attributed to the CIA. (GX809 at 8, 10, 11; Tr. 1421-28, 1604-05, 1653-55.)[5] The public release of this kind of information could enable targets of CIA cyber operations to identify, not only the cyber tool used in the operation, but individuals involved in deploying the tool—risking human assets being burned, retaliated against, and potentially executed. (Tr. 1366-67.) Schulte's writings also reflect his desire to leak and cause the leak of classified information, such as hashtags "#TopSecret" and "#FuckYourTopSecret" (GX809 at 11) and exhortations to government employees to "send all your govt's secrets here: WikiLeaks." (GX809 at 13.) The information Schulte planned to disclose in his information war was not included in his classified discovery or in the WikiLeaks Disclosures.

On September 12, 2018, Schulte wrote about finalizing copy, referring to his blog posts and articles; and scheduling tweets. Schulte in fact had created a Buffer account, an application for scheduling tweets or Facebook posts (Tr. 1858), and had linked his Twitter account, "@freejasonbourne," to the Buffer account. (DX815.) One of Schulte's articles, called Article 10 or Malware of the Mind, included a description of CIA cyber tool techniques for concealing data. (GX801.) The FBI searched Schulte's MCC cell and seized the contraband phones on October 3, 2018, before Schulte publicly released his blog posts and tweets. (Tr. 1813-14.)

7. Schulte's Convictions

As a result of this conduct, in March 2020, Schulte was found guilty at trial in the Southern District of New York ("SDNY") on two counts of violating 18 U.S.C. §§ 401(3) and 1001.[6] On July 13, 2022, Schulte's second trial in the SDNY ended in a verdict of guilty on (1) four counts of violating 18 U.S.C. § 793 (espionage), in connection with his 2016 unlawful theft and transmittal of classified information from the CIA and his 2018 unlawful disclosures and attempted disclosures of classified information from the MCC; (2) four counts of violating 18 U.S.C. § 1030 (computer fraud), in connection with Schulte's unauthorized accessing and manipulation of CIA computer systems and theft of classified information from therein; and (3) one count of violating 18 U.S.C. § 1503 (obstructing a grand jury proceeding), in connection with false statements Schulte made to the FBI during its investigation. Finally, on September 13, 2023, Schulte's third trial in the SDNY ended in a verdict of guilty on charges of receiving, possessing, and transporting child pornography, in violation of 18 U.S.C. § 2252A.[7] Sentencing on all counts of conviction is scheduled for February 1, 2024.

---

[5] In addition to Schulte's planned disclosures about Bartender, his planned internet posts contained classified information about other CIA operations, the particulars of which remain classified, and which were not derived from classified discovery or the WikiLeaks Disclosures.

[6] The jury failed to reach a verdict on the remaining counts in the first trial.

[7] SDNY elected not to proceed to trial on a separate count of violating 18 U.S.C. § 2319, in connection with Schulte's criminal violation of copyrights. Additionally, on August 29, 2023, the

8. The Imposition of SAMs

On October 26, 2018, SAMs were imposed on Schulte based on his repeated disclosures and attempted disclosures of classified information and protected discovery materials. The SAMs, broadly speaking, limit his contact with other inmates and the public, allowing contact with his attorneys and monitored visits by family members. (D.E. 92 Ex. F). The SAMs were not imposed solely on the basis of Schulte's conduct at the CIA that led to his original charges for crimes of espionage—they were only imposed after he subsequently committed crimes (for which he has been convicted at trial) of disclosing and attempting to disclose *additional* sensitive national defense information while incarcerated in general population at the MCC.

The SAMs were imposed, and have been renewed each year, consistent with the provisions of the Code of Federal Regulations and the Justice Manual ("JM") governing such restrictions. From their inception, the SAMs have been justified each year by a "written certification to the Attorney General by the head of a member agency of the United States intelligence community that the unauthorized disclosure of such information would pose a threat to the national security and that there is a danger that the inmate will disclose such information." 28 C.F.R. § 501.2(a). That certification has been accompanied by a written memorandum from the U.S. Attorney for the Southern District of New York to the Director of the Department of Justice's Office of Enforcement Operations explaining, among other things, "why special measures should be implemented." JM 9-24-100. Nor is renewal an automatic process. Not only must the relevant agency head—in this case the Director of the CIA—personally recertify that there continues to be "a danger that the inmate will disclose classified information and that the unauthorized disclosure of such information would pose a threat to the national security," 28 C.F.R. § 501.2(c), but also requires the U.S. Attorney to address "whether the circumstances identified in the last request to the Attorney General for special administrative measures have changed and, if so, what changes are recommended either to tighten up or loosen the restrictions," JM 9-24-200. These procedures have been followed with each annual renewal of the SAMs in this case, most recently in October 2023.

During the pendency of the Schulte prosecution, the SDNY Court has twice found that the SAMs imposed on Schulte are justified. On May 10, 2019, Schulte, through his attorneys at the time, moved to vacate the SAMs imposed on October 26, 2018, arguing that the SAMs were unconstitutional and not reasonably necessary to prevent the disclosure of classified information. *See United States v. Schulte*, 17 Cr. 548 (JMF) (S.D.N.Y.) (D.E. 92). On August 14, 2019, Judge Crotty largely denied Schulte's motion, granting the motion only in limited respects regarding certain communications involving non-attorney members of his legal team and monitored contacts with non-immediate family members. (*See* D.E. 127.)

It is incorrect to assert, as petitioner's counsel has, that Judge Crotty's order "relie[d] exclusively on [Schulte's] access to information while incarcerated." (Tr. of 12/18/23 Conf. at 11.) In that Order, Judge Crotty made clear that the SAMs were warranted based on Schulte's pattern

---

current presiding District Judge, the Honorable Jesse M. Furman, granted Schulte's motion for a judgment of acquittal as to the violation of 18 U.S.C. § 1503 only.

of escalating disclosures, which were not limited to information contained in classified discovery, and the continued threat posed by Schulte to disclose more sensitive and classified information:

> The SAMs are undoubtedly restrictive, but generally they are reasonably necessary to avoid further disclosure of classified information. Despite escalating restrictions on Schulte's freedom prior to his isolation in 10 South, Schulte continued to flout Court orders and his bail conditions, protective order, BOP rules, and procedures for handling classified information. If the Government's allegations against Schulte are true, Schulte intended to engage in an information war which would involve leaking classified information to the news media. Restrictive measures needed to be placed on Schulte to prevent unauthorized disclosure of classified information. (D.E. 127 at 8.)

On June 24, 2021, Schulte, again through his then-attorneys, filed a second motion to vacate the SAMs, in which his arguments were substantially similar to those he had made in his first motion. (*See* D.E. 474.) On October 6, 2021, Judge Crotty denied Schulte's motion in its entirety. (*See* D.E. 527.) The SDNY Court held that Schulte had "failed to undermine the original factual underpinnings for the SAMs." *Id.* Rather, "[t]o the contrary, since the SAMs were imposed, Schulte, *inter alia*, has been convicted of violating this Court's protective orders, and has intentionally disclosed information he knows to be classified—including in a recently publicly-filed motion seeking declassification of that very information." *Id.*[8] Accordingly, the SDNY Court held, "as it did in 2019, that the SAMs are justified by a demonstrable danger that Schulte will disclose classified information." *Id.* (alterations and internal quotation marks omitted). Indeed, Judge Crotty specifically rejected the suggestion that changed circumstances warranted removal of the SAMs, noting that "these measures, although hard, are reasonably related to legitimate penological objectives," citing not merely the fact that Schulte was "handling and reviewing sensitive classified material in discovery as he prepares his pro se defense," but also that Schulte was "continuing his troubling pattern of disrespect for the Court's protective orders and other directives regarding classified information." *Id.* at 3. Schulte appealed Judge Crotty's ruling; the Government moved for summary affirmance of Judge Crotty's ruling upholding the SAMs, which the Second Circuit granted on December 15, 2022. *United States v. Schulte*, No. 21-2877, Dkt. 142 (Dec. 15, 2022), *cert. denied*. June 26, 2023.

Similar issues regarding the danger to the public posed by the threat of Schulte's continued unauthorized disclosure of classified information arose in the context of Schulte's renewed application for bail. (D.E. 544.) The SDNY Court denied the motion for bail in an oral ruling at a conference in the case on December 20, 2021, concluding that "there is overwhelming evidence . . . that Mr. Schulte poses a danger to the community" warranting his continued detention. (12/20/21 Tr. at 66.) On May 3, 2022, the Second Circuit affirmed the SDNY Court's denial of Schulte's renewed bail application. *United States v. Schulte*, 2022 WL 1316210, at *2-4 (2d Cir. May 3, 2022). In so ruling, the Second Circuit "discussed—and endorsed—the district court's

[8] Schulte filed the motion to which the SDNY Court referred in its order in or about September 2021. The SDNY Court has since removed the motion from the public docket. *See id.* at 2 n.2.

thorough analysis of the 'overwhelming evidence' of Schulte's dangerousness, taking into account the 'sophisticated theft and dissemination of highly classified information, his violations of protective orders, and his continued disclosures and attempted disclosures of classified information, even from jail.'" *Id.* at *2-4. Indeed, by returning a guilty verdict against Schulte on July 13, 2022, the jury found beyond a reasonable doubt that Schulte engaged in, among other things, disclosing and attempting to disclose classified information, even from jail.

9. Schulte's Continued Abuse of Electronics and Threats to Disclose Classified Information

Schulte's recent conduct leading up to and during his second trial regarding the largest disclosure of CIA classified material in the history of our nation continues to demonstrate his ability and intention to circumvent the SAMs and disclose additional classified information. For instance, Schulte's discovery laptop at the Metropolitan Detention Center ("MDC")[9] had evidence of unauthorized usage, including changes to the system BIOS settings and the creation of a large, encrypted partition, which led a magistrate judge to issue a warrant authorizing the FBI to seize and search the laptop. As a result of that review, the FBI found multiple files depicting child pornography, as well as forensic artifacts reflecting that files containing child pornography had been accessed from Schulte's prison discovery laptop at MDC, including during his 2022 trial. Relevant parts of the FBI's preliminary findings were described in a declaration filed before Judge Furman on August 7, 2023. (D.E. 1093, attached as Exhibit B; *see also* D.E. 1094 ("In the Court's view, this filing should, once and for all, put to rest any contention that Defendant was or is entitled to a laptop in connection with preparing for his next trial.").)

Schulte has also repeatedly threatened to disclose classified information in his various post-trial filings. In January 2023, Schulte filed a Rule 29 motion describing how he "retains so much real national defense information that would be extremely damaging to the national security of the United States." (D.E. 992 at 23-24.) In that same filing, Schulte wrote, "If and when Mr. Schulte ever decides to wage a war against the United States, he could easily cause true, catastrophic damage." (*Id.*) Similarly, in May 2023, Schulte filed a letter complaining about lack of access to a sensitive compartmented information facility ("SCIF"), and claimed that "if the Court prevents Mr. Schulte from using the SCIF to write potentially classified information or from bringing his material to be reviewed by standby counsel in the SCIF, then the protective order is essentially null and void – and neither the court nor the government can blame or take action against Mr. Schulte for any incidental disclosure of classified information." (D.E. 1040.)

10. Continued Necessity of the SAMs

As set forth above, Schulte has repeatedly disclosed, attempted to disclose, and threatened to disclose sensitive national defense information even while incarcerated. As certified by the Director of the CIA as recently as October 2023, that remains an ongoing concern. The parties stipulated at trial in 2022 that Schulte "remains aware of sensitive national defense information beyond what he is charged with disclosing or attempting to disclose . . . , the disclosure of which would be extremely damaging to national security." (Exhibit A.) As the stipulation makes clear,

[9] Schulte was transferred from the MCC to the MDC in late 2021.

that information is not limited to that which was produced in classified discovery or that he was charged with disclosing. For example, Schulte remains aware of the true identities of undercover CIA officers with whom he worked (and some of whom testified at his trials pursuant to extensive security measures authorized by the SDNY Court to protect their identities (*see* D.E. 293, 825 at 4-5). There is no question that the protection of this information from unauthorized disclosure is a legitimate penological interest. *See, e.g.*, *Haig v. Agee*, 453 U.S, 280, 307 (198l) (explaining that "[m]easures to protect the secrecy of our Government's foreign intelligence operations plainly serve" national security interests); *Snepp v. United States*, 444 U.S. 507, 510 n.3 (1980) ("The Government has a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service."); *United States v. Sterling*, 724 F.3d 482, 516 (4th Cir. 2013) ("The identity of CIA operatives is, and always has been, subject to rigorous protection."). And the necessity of the SAMs governing Schulte's continued custody is illustrated most clearly by the fact that he stands convicted for committing and attempting to commit the very sorts of unauthorized disclosures of classified information that the SAMs are designed to guard against. *See, e.g.*, *United States v. Guzman Loera*, 24 F.4th 144, 154 (2d Cir. 2022) ("[T]he risk to prison guards and other inmates if Guzman were placed in the general population is also supported by the Government's evidence that he previously bribed prison officials and attempted to harm cooperating witnesses."); *United States v. Felipe*, 148 F.3d 101, 111 (2d Cir. 1998) ("From his jail cell, Felipe committed the very crimes for which he is now serving a life sentence. And, until shown differently, we agree with the district court's observation that, given the opportunity, appellant would likely continue such illegal activity.").

Given the sophistication of Schulte's crimes, his demonstrated capability to evade restrictions on his use of electronic devices, and his repeatedly professed willingness—indeed, desire—to disclose classified national defense information in order to harm those that he perceives as having wronged him (*see* Tr. 685 (noting that Schulte was "making clear to the jury that even today you remain aggrieved")), no other alternative would suffice. *See, e.g.*, *United States v. El-Hage*, 213 F.3d 74, 82 (2d Cir. 2000) ("The alternative to El-Hage's current confinement conditions appears to be his confinement as part of the general prison population. Because his dangerousness arises out of the information he might communicate to others, it was reasonable for the government to find that alternative unacceptable."). Indeed, Schulte has proven his ability to evade the less restrictive measures initially in place to constrain his unauthorized disclosures of sensitive national defense information. *Cf. Felipe*, 148 F.3d at 110 ("Appellant has shown himself to be resourceful in the past; it cannot now be definitely determined that he will refrain from using apparently 'innocent' privileges—e.g., sending a picture to a magazine art contest—to order the commission of a violent act, with or without the recipient's awareness.").

Schulte stands convicted of the largest theft and dissemination of classified information in the history of the CIA. He doubled down on that offense by committing and attempting to commit further unauthorized disclosures, for which he has also been convicted. His behavior while incarcerated has shown a clear pattern of disregard for court orders, a willingness to disclose further classified information, and a penchant for creativity in evading the restrictions placed upon him. All the while he remains aware of a range of sensitive classified information that he acquired through his work at the CIA, and that he poses a continued risk of disclosing, potentially causing further grievous harm to national security. The SAMs renewals have been predicated on those

undeniable facts, and there is no basis—particularly in this procedural posture—for the Court to disturb them. The Government respectfully submits that Schulte's challenge to the imposition and implementation of the SAMs can and should be denied.

Respectfully submitted,

DAMIAN WILLIAMS
United States Attorney

by: */s/*
David W. Denton, Jr. / Michael D. Lockard /
Nicholas S. Bradley
Assistant United States Attorneys
(212) 637-2744/2193/1581

Enclosures